Attachment 1 - NMCI Statement of Objectives 1
1.0 Introduction 1
1.1 Definitions 1
2.0 NMCI Service Delivery Points (SDP) 1
2.1 Data Seats 2
2.2 Voice Seats 2
2.3 Video Seats 4
2.4 NMCI Infrastructure Service Delivery Points 5
2.6 External Networks 6
3.0 NMCI Services 7
3.1 Basic User Services (Not optionally orderable) 7
3.1.1 Standard Office Automation Software 7
3.1.2 E-mail Services 7
3.1.3 Directory Services (DS) 8
3.1.4 Web Access and Proxy and Caching Services 9
3.1.5 News Group Services 9
3.1.6 Multimedia Capabilities Services 9
3.1.7 Print Services 9
3.1.8 NMCI Intranet Performance 10
3.1.9 NIPRNET Access 10
3.1.10 Internet Access 10
3.1.11 Mainframe Access 10
3.1.12 Desktop Access to Government Applications 11
3.1.13 Moves, Adds, and Changes (MACs) 11
3.1.14 Software Distribution and Upgrades 12
3.1.15 User Training 12
3.1.16 Public Key Infrastructure (PKI) Integration 13
3.1.17 Un-classified Remote Access Service 13
3.1.18 Mobile Voice Messaging 13
3.1.19 Web Hosting 13
3.1.20 External Networks 14
3.1.21 Shared File Services 14
3.1.22 Retention of DON Electronic Records 14
3.2 Help Desk Services 14
3.3 Communications Services 14
3.3.1 Wide Area Network (WAN) Connectivity ..... 15~~1514~~
3.3.2 Local Area Network (LAN) and Base Area Network (BAN) Communication Services.. 15
3.3.3 Proxy and Caching Service 15
3.4 Systems Services 15
3.4.1 Network Management System (NMS) Service 15
3.4.2 Operational Support Services (OSS) ..... 16~~1615~~
3.4.3 Capacity Planning 16
3.4.4 Domain Name Server (DNS) 16
3.4.5 Search Engine Services 16
3.4.6 Data Reporting 17
3.5 Information Assurance Services 19
3.5.1 NMCI Security Operational Services 19
3.5.2 NMCI Security Planning Services 20
3.6 Other Services 20
3.6.1 Integrated Configuration Management (CM) 20
3.6.2 Integration and Testing ..... 21~~2120~~

3.6.3 Transition Planning Support 21
3.6.4 Interoperability Test Plan 21
3.7 Additional Requirements for Embarkable Seats 24
4.0 Information Assurance/Computer Network Defense (IA/CND) Requirements 26
4.1 General DoD and DoN IA Policies 26
4.2 Public Key Infrastructure (PKI) 27
4.3 Multi-Level Security (MLS) 27
4.4 Computer Network Defense (CND) 28~~2827~~
4.5 Critical Government Roles with respect to IA/CND 28
4.6 Secure Voice Interface 29
4.7 Classified (DoD) Information Support 30
4.8 Sensitive Information Support (Non-Classified) 30
4.9 Privacy and Security Safeguards 31
4.10 Certification and Accreditation (C&A) 31
4.11 NMCI Enclaves 32
~~Attachment 1 - NMCI Statement of Objectives 1~~
~~1.0 Introduction 1~~
~~1.1 Definitions 1~~
~~2.0 NMCI Service Delivery Points (SDP) 1~~
~~2.1 Data Seats 2~~
~~2.2 Voice Seats 2~~
~~2.3 Video Seats 4~~
~~2.4 Infrastructure Service Delivery Points 5~~
~~2.5 Organization SDPs 6~~
~~2.6 External Networks 6~~
~~3.0 NMCI Services 7~~
~~3.1 Basic User Services (Not optionally orderable) 7~~
~~3.1.1 Standard Office Automation Software 7~~
~~3.1.2 E-mail Services 7~~
~~3.1.3 Directory Services (DS) 8~~
~~3.1.4 Web Access Services 9~~
~~3.1.5 News Group Services 9~~
~~3.1.6 Multimedia Capabilities Services 9~~
~~3.1.7 Print Services 9~~
~~3.1.8 NMCI Access **Error! Bookmark not defined.**~~
~~3.1.9 NIPRNET Access 10~~
~~3.1.10 Internet Services 10~~
~~3.1.11 Mainframe Access 10~~
~~3.1.12 Desktop Access to Legacy Applications 10~~
~~3.1.13 Moves, Adds, and Changes (MAC) 11~~
~~3.1.14 Software Distribution and Upgrades 11~~
~~3.1.15 User Training 11~~
~~3.1.16 Public Key Infrastructure (PKI) Integration 12~~
~~3.1.17 Non-classified Remote Access Service 12~~
~~3.1.18 Mobile Voice Messaging 12~~
~~3.1.19 Web Hosting 13~~
~~3.1.20 External Networks 13~~
~~3.1.21 Shared File Services 13~~

~~3.2 Help Desk Services .... 13~~
~~3.3 Communications Services .... 13~~
~~3.3.1 Wide Area Network (WAN) Connectivity .... 13~~
~~3.3.2 Base Area Network (BAN) Communication Services .... 14~~
~~3.3.3 Proxy and Caching Service .... 14~~
~~3.4 Systems Services .... 14~~
~~3.4.1 Network Management System (NMS) Service .... 14~~
~~3.4.2 Operational Support Services (OSS) .... 14~~
~~3.4.3 Capacity Planning .... 15~~
~~3.4.4 Domain Name Server (DNS) .... 15~~
~~3.4.5 Search Engine Services .... 15~~
~~3.4.6 Data Reporting .... 16~~
~~3.5 Information Assurance Services .... 17~~
~~3.5.1 NMCI Security Operational Services .... 17~~
~~3.5.2 NMCI Security Planning Services .... 18~~
~~3.6 Other Services .... 18~~
~~3.6.1 Integrated Configuration Management (CM) .... 18~~
~~3.6.2 Integration and Testing .... 18~~
~~3.6.3 Transition Planning Support .... 19~~
~~3.7 Additional Requirements for Embarkable Seats .... 20~~
~~4.0 Information Assurance/Computer Network Defense (IA/CND) Requirements .... 22~~
~~4.1 General DoD and DoN IA Policies .... 22~~
~~4.2 Public Key Infrastructure (PKI) .... 22~~
~~4.3 Multi-Level Security (MLS) .... 23~~
~~4.4 Computer Network Defense (CND) .... 23~~
~~4.5 Critical Government Roles with respect to IA/CND .... 24~~
~~4.6 Secure Voice Interface .... 25~~
~~4.7 Classified (DoD) Information Support .... 25~~
~~4.8 Sensitive Information Support (Non-Classified) .... 26~~
~~4.9 Privacy and Security Safeguards .... 27~~
~~4.10 Certification and Accreditation (C&A) .... 27~~
~~4.11 NMCI Enclaves .... 27~~

Attachment 1 - NMCI Statement of Objectives

1.0 Introduction

This document represents those requirements, that have not otherwise been identified in the solicitation. All services provided shall meet the levels of service specified in Attachment 2.

Where unpriced options are exercised by NMCI customers, their accompanying description of services will be developed using the SLAs contained in Attachment 2 as the entering baseline. The resulting description of services will include any adds or changes to accommodate additional or customer specific requirements.

1.1 Definitions

For the purposes of this document, the following definitions apply:

Assurance refers to availability, restricted access/confidentiality, integrity/data quality, attack/intrusion detection time, and attack termination time.

Capacity refers to ubiquity of access, connectivity, redundancy/diversity, compute capacity, committed information rate/peak information rate, and growth potential/scalability.

Legacy System refers to a hardware and/or software system that consists in whole (or part) of legacy applications, or uses legacy applications to achieve its transport or enabling capability.

Legacy Application refers to a software program typically developed for use on an internal corporate network without the application designers having full awareness of the requirements to accommodate the application for compatibility with wide-area network environment.
Network Operation Center (NOC): Anywhere throughout this or any other attachment where NOC is mentioned, Network Management Center (NMC) also applies. NMC falls under the cognizance of COMSIXTHFLT.
Responsiveness refers to latency, throughput, training, interoperability, customer service, adaptability to stress, restoration time, time to increase/enhance capability, and technical refresh rate.

User Account refers to access to the service exclusive of the hardware and LAN drop. User accounts will be aggregated at the NMCI enterprise level.

2.0 NMCI Service Delivery Points (SDP)

The NMCI contractor shall provide services with security features to a range of Navy and Marine Corps end points that include data, voice, and video users, the general NMCI enterprise infrastructure, and interfaces to other DoN and DoD communications environments. The NMCI contractor shall also provide support to non-DoN end points that are identified as users of those services under the current data and voice networks/systems.

The service delivery points for users include access to a specific set of basic data, voice, or video services that are required to provide the specified SDPs (Service Delivery Points) capability and associated services. The user SDPs are defined as follows:

2.1 Data Seats

A data seat is comprised of the hardware, software, security features and services provided to the NMCI user as computing resources. The data seats are defined as fixed workstation, portable, embarkable, embarkable portable, and hybrid. Each of these is available in a basic configuration, and with the exception of the hybrid seat, is available with upgrades to support high-end, mission-critical, and/or classified functionality.

Two user accounts are included with each non-classified data seat. User accounts can be accessed from any NMCI workstation.

The fixed workstation represents the baseline configuration with respect to software. Capabilities and functions that the contractor shall provide as a baseline configuration are defined in 3.0 and shall include but not be limited to: e-mail, web access, web hosting service, standard office automation, collaboration tools, file sharing, printing services, newsgroup services, multimedia capabilities, NMCI access, NIPRNET access, directory services, mainframe access, desktop access to legacy applications, software distribution and upgrades, user training, PKI integration, non-classified remote access service, help desk, integrated configuration management, and integration and testing. Software applications are intended to support Naval Business processes and shall include a technology refreshment rate as improvements or upgrades become available and in accordance with industry "best practice" and the terms and conditions of this contract. The NMCI contractor shall provide desktop system drivers to facilitate the configuration of the user workstation, or seat, which is provided as a service of NMCI.

To achieve the IA goals within the Department of the Defense (DoD), a smart card reader will be necessary with Public Key Infrastructure (PKI) enabled applications to access DoD PKI credentials. The Contractor shall provide a smart card reader with each data seat in accordance with the Smart Card reader requirements in Attachment 8. DoN will provide smart cards as GFE. The Contractor shall provide data seats with the capability, including all required software, of supporting Smart Cards in accordance with the Smart Card reader requirements in Attachment 8.

2.2 Voice Seats

The contractor shall provide users with voice communication services. ~~After contract award~~As voice services are transitioned to NMCI, operations, maintenance and disposal (when required) of the associated existing voice infrastructure shall be the responsibility of the contractor. Existing voice infrastructure includes but is not limited to outside/inside cable plant, associated ducts, manholes, aerial support structures, air pressurization systems, voice microwave systems, PBX switching equipment, key service units, telephone instruments, distribution frames, generators, and associated power conditioning equipment. If the Contractor transitions legacy voice systems to services integrated with data, the Contractor shall maintain voice SLA performance requirements.

Reference: SLA 22

2.2.1 Description of Voice Seats, Upgrades and Services

a. **Basic Voice Seat:** Non-secured voice communications provides the user access to voice communications with basic services. A fixed voice service seat includes instruments, infrastructure, and other services to provide non-secured telephone-related connectivity within and external to NMCI. The basic capabilities/services are call forwarding, call transfer, call hold, call waiting, call pickup, and hunt group. Voice seat service also includes user training, help desk, integrated configuration management, and integration and testing. The contractor shall provide for connecting users to voice communication service. The basic voice seat price includes unlimited local Public Switch Telephone Network (PSTN) usage and unlimited calls to NMCI voice seats. Basic voice seat capabilities include interoperability with Defense Switched Network (DSN), Federal Telecommunications System (FTS) 2001 and Government Emergency Telecommunications System (GETS). The DSN interoperability of the Basic Voice Seat shall also support Multi Level Precedence and Preemption (MLPP), and end user MLPP interactions shall be provided in accordance with DISA JIEO technical report 8249 (GSCR) paragraph 2.2.1 and subparagraphs. The Contractor shall provide operator services to include directory assistance (i.e., 411), enhanced 911 capabilities, and 24 hour operator-assisted calling, including DSN OCNUS calls.

b. **Business Voice Seat Upgrade**: A business voice seat upgrade adds a premium voice terminal with the following additional features beyond the requirements of a basic voice seat: voice mail, caller-id, and conference calling (minimum 3 party conference).

c. **Mission Critical Voice Seat Upgrade**: A mission critical voice seat upgrade package increases availability of service.

d. **Pier Voice Line**: A pier voice line provides voice connectivity for ships pierside at designated Navy and Marine Corps facilities. The contractor provided connectivity shall interface with government provided ship's telephones or telephone equipment. The pier voice line provides the same NMCI capabilities/services that are associated with the Basic Voice Seat, and the pier voice line price includes unlimited local PSTN access and unlimited calls to NMCI voice seats. The contractor shall provide the capability to provision pier voice lines within 24 hours (normal) or 1 hour (emergency).

e. **Pier Voice Trunk**: A pier voice trunk (DS0s bundled into DS1s) provides voice connectivity for PBX-equipped ships pierside at designated Navy and Marine Corps facilities. The contractor provided connectivity shall interface with government provided ship's telephone equipment. The pier voice trunk provides the same NMCI capabilities/services that are associated with the Basic Voice Seat, and the pier voice trunk price includes unlimited local PSTN access and unlimited calls to NMCI voice seats. The contractor shall provide the capability to provision pier voice trunks within 24 hours (normal) or 1 hour (emergency).

f. **Commercial Voice Seat**: Commercial voice seat provides voice services to commercial entities, family housing and unofficial users located on Navy and Marine Corps installations where ready connection to the Public Switched Telecommunications Network (PSTN) is not available. The provision and cost of this service shall be in accordance with DoD policy for class B service defined in DoD Directive 7220.9-M. The NMCI Commercial Voice seat only provides unlimited calls within the local calling area. The contractor shall also provide the Commercial voice seat with access to commercial long distance carriers.

g. **Commercial Voice Connectivity**: Commercial voice connectivity provides communications infrastructure to commercial entities, family housing and unofficial users located on Navy and Marine Corps installations for connection to the Public Switched Telecommunications Network (PSTN).

2.2.2 Voice Demarcation Points. The Government shall provide trunks to connect to the DSN, however, the contractor shall provide interface ports in accordance with the ICD. The contractor shall provide all trunking to the PSTN and FTS networks to meet the required Grade of Service (GOS). The contractor shall also provide voice service via designated SDP for underway or forward deployed units/platforms. This service will be delivered via analog lines, DS0 or DS1 services.

2.2.3 Billing. The contractor price for the Basic Voice Seat, the Pier Voice Line, and the Pier Voice Trunk shall include unlimited local PSTN access (including local toll costs) and unlimited calls to other NMCI voice seats. Calls to off-net locations shall be routed over the NMCI to the NMCI location nearest the destination point. The contractor shall route calls over the DSN or FTS only when specified by the user on a per call basis. The contractor shall prepare separate billing statements at the seat/line/trunk level for tolls associated with use of FTS-2001 or commercial long distance charges for calls to non-NMCI users. The government shall be responsible for certifying bills, resolving billing disputes and collection of payments.

2.2.4 Minimum Voice Mail Specifications. **Integrated Voice Messaging System (IVMS).** IVMS shall be provided to meet the requirements provided below. The IVMS shall provide, at a minimum, the following features:

a. Interaction with DTMF signaling.
b. User security via password.
c. Administrative capability to increase and decrease maximum message length.
d. Notification of the number of messages waiting to be processed when each subscriber accesses the system.
e. User overridable voice prompts providing instruction on usage of the IVMS.
f. User review of message(s) before release, with options to edit only, send, and delete.
g. User transmission and receipt of messages for optional access and storage for future retrieval.
h. Notification of non-delivery of messages.
i. Audible confirmation of message transmission date and time.
j. Four user-accessible distribution lists with up to 100 addressees.
k. Call answering with personal greeting.
l. Call transfer and an escape feature.

The Contractor shall provide an Integrated Voice Messaging System. Each IVMS shall provide voice messaging transmission, reception, and voice message storage 24 hours-per-day, seven days-per-week, 365 days-per-year except for periodic maintenance downtime. Each IVMS shall be interoperable with the DSN and shall provide a P.05 grade of service to its subscribers. Phone sets will advertise waiting messages visually.

Scope: All voice seats and data seats with voice capability.

SLA 22A

2.3 Video Seats

These services shall consist of high bandwidth communications, point-to-point, and continuous transmission that allows participants to conduct visually interactive electronic meetings between one or more distant locations using video cameras, monitors, and audio and video communications, thus enabling participants to see and hear each other as if they were in the same room. Some of the features of this equipment shall include but not be limited to: room cameras with full area coverage, large monitors, on-screen menus, dynamic speaker technology, far end camera control, video player/recorder capability, software distribution and upgrades, user training, help desk, integrated configuration management, integration and testing, and remote diagnostics.

2.3.1 Description of Video Seats, Upgrades and Services

h. **Basic and High End Video Seat:** Secured (Type 1 encrypted video transmission – i.e. KIV-7 HS, KG-194) and non-secured video communications provides the user access to video communications with basic services. A fixed or moveable video service seat includes instruments, infrastructure, and other services to provide non-secured video-related connectivity within and external to NMCI. Video seat service also includes user training, help desk, integrated configuration management, and integration and testing. The contractor shall provide for connecting users to video communication services including. The basic video seat price includes unlimited VTC usage between NMCI users. Basic video seat capabilities include interoperability with DISN Video Services - Global (DVS-G), Federal Telecommunications System (FTS) 2001, ISDN and other commercial digital services. The contractor shall provide operator services to include operator-assisted VTC setup and operation including off-hour support.

i. **Mission Critical Video Seat Upgrade**: A mission critical video seat upgrade package increases availability of service and operation assistance.

j. **Video Demarcation Points.** The Government will provide trunks to connect to the DSVG, however, the contractor shall provided interface ports in accordance with the ICD. The contractor shall provide all trunking to the PSTN and FTS networks. The contractor shall also provide video service via designated SDP for forward deployed units/platforms. This service will be delivered via ISDN or other digital transmission services. The pier video service provides the same NMCI capabilities/services that are associated with the Fixed Video Seat, and the pier video service includes unlimited calls to other NMCI video seats. Video calls to off-net locations shall be routed over the NMCI to the NMCI location nearest the destination point.

k. **Billing**: The contractor price for the Basic and High End Video Seats shall include unlimited (including tolls or line costs if any) VTCs to other NMCI video seats. Calls to off-net locations shall be routed over the NMCI to the NMCI location nearest the destination point. The contractor shall route calls over the DSVG or FTS only when specified by the user on a per call basis. The contractor shall prepare separate call detail reporting billing statements at the seat level for tolls associated with use of DSVG, FTS-2001, or commercial long distance charges for calls to non-NMCI users. The government shall be responsible for certifying bills, resolving billing disputes and collection of payments.

Scope: All Fixed and moveable VTC seats.

SLA 26

2.4 NMCI Infrastructure Service Delivery Points

The contractor shall provide at no additional cost to the Government enterprise infrastructure services that are transparent to the NMCI service area and OCONUS (if option is ordered) users but are essential to NMCI functionality, security, performance, and interoperability. If OCONUS services are not ordered, the Contractor shall make technical information available to the OCONUS provider to ensure interoperability between NMCI and OCONUS users. "Infrastructure services" refer to the various management/operational activities, hardware, software, and transmission medium necessary for the delivery of services to NMCI users. Infrastructure shall include connectivity and transport services to IT-21 provisioned piers and IT-21 NOCs within the NMCI service area, and the MCEN NOC in accordance with the NMCI Interface Control Document (Attachment 10).

Scope: All seats

2.5 Additional Organization Services

These additional services can be ordered on an organizational level:

2.5.1 Optional User Capabilities, Clin 0023 (and 0123 if option is exercised)

2.5.2 Additional services above those provided as a basic service:

Additional Shared File Services, Clin 0016 (and 0116 if option is exercised)
Additional Unclassified Account, Clin 0024 (and 0124 if option is exercised)
Additional Classified Account, Clin 0025 (and 0125 if option is exercised)
Additional Moves, Adds, and Changes (MAC), Clin 0026 (and 0126 if option is exercised)

Services negotiated on an individual order basis:

Application Server Connectivity, Clin 0027 (and 0127 if option is exercised)
Data Warehousing, Clin 0028 (and 0128 if option is exercised)
Legacy System Support, Clin 0029 (and 0129 if option is exercised)

2.6 External Networks

The Contractor shall provide connectivity with DISN (NIPRNET and SIPRNET), MCTN, IT-21, and Internet and other networks as specified in Attachment 10. The Contractor shall provide sufficient bandwidth to meet performance specifications as stated in Attachment 2 and security features as specified in Attachment 4. This requires seamless interface with the established communications systems that support DoN as well as Joint Forces in operational environments. Contractor shall provide infrastructure to DISN Points of Presence (POP) and any additional infrastructure necessary to meet required service levels (Attachment 2). Use of the DISN does not obviate the requirement for the Contractor to perform in accordance with Attachment 2. Commercial alternatives must be approved by the Government prior to implementation.

DISN long-haul services will be provided to the Contractor by the Navy at no cost to the Contractor. DISA will provide DISN WAN SLAs necessary for the Contractor to reach decisions on design solutions that meet NMCI required service levels. DISN SLAs will be negotiated between DISA and DoN based on detailed traffic flow requirements provided by the contractor during transition planning for the ordered increment. During Contract performance, DISA will have the first opportunity to provide all WAN requirements deemed necessary by the Contractor, and the Contractor may request Government waiver if commercial or other alternatives are necessary. Commercial solutions must meet interoperability and security requirements of DoD. If in meeting its obligation to satisfy the NMCI end-to-end performance, the Contractor requires enhancement to standard DISN performance, the Contractor shall provide the analysis and justification sufficient to support a waiver to the DoD long haul telecommunications policy. Upon approval of said waiver, the Contractor shall coordinate the engineering and installation of the Contractor’s e infrastructure components and/or services with the DON . DON will provide for the requisite coordination with DISA.

Reference: SLA 27

3.0 NMCI Services

The NMCI Service Elements are arranged in six Service Categories. These categories include User Support Services, Maintenance Services, Help Desk Services, Communications Services, Information Assurance Services, and Advanced Application and IM Support. A large percentage of these services are necessary to provide basic NMCI functionality and are included in all as “Basic Services”. Some of these services are for specific customers and may not be provided to the general user population, and are included as “Optional Services”.

Each of the six Service Categories is described here, with their constituent Service Elements. For each, there is a brief description of the service followed by a list of notional performance measures that may be used by the Government in evaluating contractor performance in delivery of that service to the NMCI customer.

3.1 Basic User Services (Not optionally orderable)

3.1.1 Standard Office Automation Software

Requirement: The standard desktop integrated software suite shall include word processing, spreadsheet, presentation graphics, database, and support a collaborative work environment.

COTS software beyond that provided as standard office automation will be available and purchased separately under Item 0023 (COTS catalog).

Scope: Basic service requirement for all data seats with the exception of the Basic Hybrid Seat, which requires only standard office automation viewer software.

Scope: Basic service requirement for all data seats with the exception of the basic hybrid seat, which requires only standard office automation viewer software.

Reference: SLA 2

3.1.2 E-mail Services

Requirement: The contractor shall provide services for sending, storing, processing, and receiving e-mail and multi-media e-mail attachments, with interoperability across DoN and within the DoD. The services shall be configurable to provide Medium Grade Service (MGS) capability for sending and receiving signed and encrypted e-mail and attachments, by utilizing DoD PKI (Public Key Infrastructure) issued user certificates, and interoperable with MGS systems outside the NMCI domain. . MGS shall be provided with e-mail packages that support cryptographic functions from a smart card. The contractor will ensure that foreign nationals are clearly identifiable in electronic communications in accordance with DoD Directive 5230.20

Description: A widely used Network application in which mail messages are transmitted electronically between end users over various types of networks using a variety of network protocols. An electronic means for communication in which (a) usually text is transmitted, (b) operations include sending, storing, processing, and receiving information, (c) users are allowed to communicate under specified conditions, and (d) messages are held in storage until called for by the addressee. Each seat should be supplied with E-mail capability and file transfer management tools. It is an integral part of NMCI, and shall conform to industry standards (e.g., native RPC, HTTP, IMAP4) for interoperability and remote access and DoN conventions for domain naming (i.e., retention of navy.mil and usmc.mil domains) .

Scope: Basic service requirement for all data seats. The Basic Hybrid seat only requires on-line e-mail processing capability.

Reference: SLA 3

3.1.3 Directory Services (DS)

Requirement: The contractor shall maintain global information services delivering a distributed computing environment that supports the management and utilization of file services, network resources, security services, messaging, web, e-commerce, white pages, and object-based services, across the NMCI. Information services shall include storing, updating, and publishing directory information from multiple systems and formats including e-mail addresses, commercial and DSN telephone numbers, certificates, addresses, applications, network devices, documentation, and routing information, as well as other data/resources in support of the NMCI IT environment. The contractor shall ensure directory entries conform to Government standards and provide the flexibility to include DoN users not directly supported by NMCI in directory services.

The global directory services shall be required to maintain information on users and resources. The DS should support and facilitate the following basic functions:

1. Supported by PKI authentication services, provide the capability for users, devices, and applications to discover and utilize global information services data.

2. Support the monitoring of administration and management of network resources.

3. Support the implementation of global account management and subsequent authentication and authorization to data maintained in the global directory service.

4. Support the enablement and distribution of applications.

5. Provide a proactive environment that builds and manages relationships between objects within the global directory service.

6. Support the ability for end users to interact globally (anywhere, anytime) with the network directory services in a transparent and consistent manner.

7. Operate the legacy Navy/Marine Corps White Pages until contractor-provided directory services are complete and available throughout DoN.

Scope: Basic service with all data seats, fixed and secure voice seats, and all video seats.

Reference: SLA 4

3.1.4 Web Access and Proxy and Caching Services

Requirement: The contractor shall provide the capability and features that allow users to access in-house and external web content. The contractor shall provide communication with web host servers on NMCI, SIPRNET, NIPRNET, and Internet. The contractor shall provide and maintain an opening splash screen for NMCI logon and portal access to the web content of the NMCI. Identification and Authentication (I&A) and Access Control to the NMCI as well as to DoN secure websites will occur via DoD PKI issued certificates stored on either the DoD Common Access Card (CAC) or equivalent smart card provided by the DoN.

Scope: Basic service with all data seats.

Reference: SLA 6

The contractor shall also provide the capability for caching and proxy to enhance information access and performance. This service shall provide enhancements to both internal and external web content.

Scope: Basic service with all data seats.

Reference: SLA 26A

3.1.5 News Group Services

Requirement: The contractor shall provide services for posting, reading, and processing user-determined public and private newsgroups.

Scope: Basic service with all data seats.

Reference: SLA 7

3.1.6 Multimedia Capabilities Services

Requirement: The contractor shall provide the capability to view, hear, manipulate and manage information consisting of text, graphics, images, video, and audio. This shall also include processing and rendering of the multimedia data being transferred.

Scope: Basic service with all data seats with the exception of the hybrid seat.

Reference: SLA 8

3.1.7 Print Services

Requirement: The Contractor shall provide to the end user the capability and features to produce black and white, and color hard copies of electronic documents. The ratio of users to printers is stipulated in SLA 9; where organizations require a greater number of printers to support requirements, those printers should be ordered under CLIN 0023.

Scope: Basic service with all data seats when attached to the NMCI environment.

Reference: SLA 9

3.1.8 NMCI Intranet Performance

Requirement: The contractor shall provide a point of entry for the voice, video or data device required by the user into the NMCI network, with interoperability with other DoN and DoD service delivery points. (In some instances, this point of entry may be the service delivery point for NMCI.)

Scope: Basic service for all data, voice and video seats; not applicable for personal pagers.

Reference: SLA 10

3.1.9 NIPRNET Access

Requirement: The contractor shall provide a point(s) of entry for each data seat to access the NIPRNET.

Scope: Basic service with all data seats.

Reference: SLA 11

3.1.10 Internet Access

Requirement: The Contractor shall provide point of entry for user access to the Internet.

Scope: Basic service with all data seats.

Reference: SLA 12

3.1.11 Mainframe Access

Requirement: The contractor shall provide a service to allow NMCI customers access to applications and data stored on DoN and DoD mid-tier, mainframe or super computers. This service includes the necessary hardware, software, and infrastructure that allow interface to the client. The service shall also include but is not limited to, 3270 and VT100 terminal emulation. If the mainframe is outside an NMCI firewall, the contractor shall provide the capability to access the mainframe with security features. VPNs (Virtual Private Network) shall be used as a transition approach but shall not be used as the end solution. Virtual Private Network (VPN) devices used within NMCI shall be selected and implemented in accordance with the NMCI Security Requirements (Attachment 4), specifically the VPN selection criteria document dated 18 November 1999.

Scope: Basic service with all data seats.

Reference: SLA 13

3.1.12 Desktop Access to Government Applications

Requirement: All Government off the shelf (GOTS) legacy systems and applications in operation at the time of order shall continue to function on the NMCI in accordance with Attachment 4, 5, and 10. These systems and applications include desktop-loaded applications. Additionally, server-based applications ordered under Item 0027 must continue to function.

COTS software beyond that provided by the vendor as standard office automation will be purchased separately under CLIN 0023.

This basic service does not include software re-engineering or hosting of legacy applications on contractor-provided hardware.

Scope: Basic service with all data seats; not applicable to hybrid seat.

Reference: SLA 14

3.1.13 Moves, Adds, and Changes (MACs)

Requirement: Two categories of Moves, Adds, and Changes are addressed for NMCI -- they include those relating to Embarkables and those that are User Requested. For Embarkables, the contractor shall provide Embarkable services relating to Navy and Marine Corps organization/activity movement. These include those organization/activity movements that are known in advance and scheduled in published OPORDERs or that support contingency operations and other unplanned movements. These MACs include all actions by the contractor to transition an NMCI data seat out of the NMCI domain plus those required to return that data seat to operate on the NMCI network. A move out and a return shall be counted as one move; these are separate from User Requested MACs and will count against aggregate Embarkable MACs.

User requested MACs are aggregated on the enterprise level. Embarkable MACs are also aggregated on the enterprise level. However, user requested MACs shall be aggregated and accounted for separately from Embarkable MACs.

For User Requested MACs, the contractor shall provide services to perform user-requested system hardware and software changes of data seats. This applies within a base, to networked customers, where NMCI service already exists.

Charged as MACs are the following:

- De-installation, move and re-installation, or change of data seat hardware.
- Creation and modification of a user account including email and directory services, not associated with provisioning of an ordered CLIN.

Other user requested contractor services will be required but not charged as MACs; they include:

- Acquisition and installation of any order CLIN, including all administrative actions necessary to establish contracted services.
- A seat upgrade (Items 0007-0009), and voice upgrades (Item 0010).
- A contractor periodic or unscheduled software refresh or update.

For voice seats, administrative changes are defined as user-requested changes that the contractor will perform and that do not require a visit to customer locations. These are not considered as MACs. Examples of voice seat administrative changes include:

- Change of voice mail, password, call forwarding, call transfer.
- Assignment of class of service (i.e. enable or restrict the capability of a voice seat to place local, long distance, DSN calls).
- Change of telephone number.

Scope: One user-requested MAC per year shall be provided for each ordered data, video, or voice seat. Administrative voice changes do not constitute a MAC. One embarkable MAC per year shall be provided for Items 0003 and 0004.
~~The contractor shall provide services to perform *user-requested* system hardware and software, de-installation, move and re-installation, change, and acquisition and installation of hardware. A seat upgrade (Items 0007-0009, and voice upgrades under Item 0010) is not a MAC, and does not count against the cumulative number of moves, adds, and changes allowed per year. This applies within a base, to networked customers, where NMCI service already exists.~~

~~Administrative voice changes are *user-requested* voice changes that do not require a visit to customer locations and shall be performed by the contractor. Administrative voice changes do not constitute a Move, Add or Change; and shall be performed at no additional cost as these administrative changes shall be included in the voice seat price. Examples of administrative changes include but are not limited to the assignment of class of service (i.e. enable or restrict the capability of a voice seat to place local, long distance, DSN calls) and change of telephone number.~~

~~Scope: One MAC per year shall be provided for each ordered data, video, or voice seat. Administrative voice changes do not constitute a MAC. MACs will be aggregated at the NMCI enterprise level.~~

~~Reference: SLA 15~~

3.1.14 Software Distribution and Upgrades

Requirement: The contractor shall provide the capability to distribute new and upgraded software with the method of installation distribution and schedule in accordance with best business practices. This capability includes COTS software, Government-off-the-Shelf (GOTS), custom application software, end-user and systems services, and enterprise functional servers.
Scope: Basic service with all data, voice, and video seats.

Reference: SLA 2, 16

3.1.15 User Training

Requirement: For the hybrid seat, user training is limited to distributed electronic curricula as applicable, and help desk support. For each change in services and application, the contractor shall analyze, identify and implement the form of training most effective and efficient for NMCI users. User training shall be made available as a result of the following for any data, voice, or video seat including, as a minimum:

- Initial implementation
- Implementation of a change in technology or user interface
- Identification of user knowledge shortfall, e. g. as a result of a help desk call or user invoked systems failure
- Move/Add/Change
- Annual security training requirement
- Upon ordering officer request

Scope: Basic service for all seats (data, voice, and video) and the service delivery points for NMCI infrastructure and external networks.

Reference: SLA 17

3.1.16 Public Key Infrastructure (PKI) Integration

Requirement: The NMCI shall provide for the integration and management of the DoD Public Key Infrastructure (PKI) Service, in compliance with DoN and DoD PKI security policies and guidelines. The DoD PKI Service includes directory support, registration (operation of Local Registration Authority (LRA) workstations), interface to related NMCI systems, hosting of PKI-enabled servers, and required key management services as well as PKI solutions for email, web applications, file transfer, and Virtual Private Networks. The Government will provide the contractor with the DoD PKI user profiles as GFI to be implemented within NMCI. Certification Authority (CA) functions will be performed by the government. LRA functions will be performed by the NMCI contractor. NMCI Security Requirements (Attachment 4) provides further detail for DoD PKI integration requirements.

Scope: Basic service for all data seats and the NMCI Infrastructure service delivery point.

3.1.17 Un-classified Remote Access Service

Requirement: The contractor shall provide services that allow users to access the NMCI data network from remote Locations via a local or toll-free call. The service shall provide for the identification and authentication of the user via DoD PKI Certificates on the DoD Common Access Card or equivalent smart card provided by DoN, and authorizes access to an NMCI-defined set of services, with capacity available to accommodate Navy and Marine Corps surge requirements.

Scope: Basic service for all data seats.

Reference: SLA 18

3.1.18 Mobile Voice Messaging

Requirement: The contractor shall support a wireless capability for the user to receive messages. This capability shall include the supporting service for both visual text and recorded audio.

Scope: Basic service for the mobile phone seats and personal paging service seat.

3.1.19 Web Hosting

Requirement: Web hosting is a service provided for Navy and Marine Corps web sites, including storage and processing of web content. This service includes NMCI internal access, public access, and classified hosting. As part of this service, Contractor must provide statistics regarding web access. The service does not include authoring of the web content and application development.

Scope: Basic service for all data seats

3.1.20 External Networks

Requirement: External network supports specific basic connections to other DoD networks such as MCTN and IT-21, and to major commercial partners of Navy and Marine Corps stakeholders required to support their procurement programs.
Scope: Basic service for all data seats

3.1.21 Shared File Services

Requirement: This service allows users to store and retrieve files on shared, controlled access storage media. This includes access controls, and back up and recovery.

Scope: Basic service for all data seats

3.1.22 Retention of DON Electronic Records

Requirement: The contractor shall provide retention of electronic information files consistent with applicable DoD (DoD Standard 5015.2-STD) and DON policy (SECNAVINST 5212.5D).

Scope: Basic service for all data seats

3.2 Help Desk Services

Requirement: The contractor shall provide user technical assistance for solving NMCI issues to the user's satisfaction. This includes integrated service provider, and shall be the single point of contact for all NMCI users. The user shall have the capability to interact or communicate with the help desk by voice, email, and/or by fax; additionally designated users shall have visibility into a web-based trouble ticket status system. These capabilities also include the timely notification by the help desk of planned or unplanned system maintenance or degradation of the NMCI.

Scope: Basic service for all user accounts.

Reference: SLA 23

3.3 Communications Services

Requirement: The contractor shall provide communications services with security features in accordance with the requirements in the following subparagraphs.

3.3.1 Wide Area Network (WAN) Connectivity

Requirement: The contractor shall provide all services required to attain wide area network (WAN) connectivity between geographically separated Navy and Marine Corps users/devices. It provides connection to external networks, to include but not be limited to: Non-Secure IP Router Network (NIPRNET), Secure IP Router Network (SIPRNET), Defense Research Engineering Network (DREN), Defense Switched Network (DSN), Public Switched Telephone Network (PSTN), and the Internet. The NMCI Interface Control Document (ICD) (Attachment 10) provides the interface requirements applicable for WAN connectivity. The WAN solution shall incorporate the Government-Service Provider agreement for DISA connectivity.

Scope: Basic service for NMCI infrastructure, and external networks

Reference: SLA 24

3.3.2 Local Area Network (LAN) and Base Area Network (BAN) Communication Services

Requirement: The contractor shall provide the capability to interconnect geographically co-located Navy and Marine Corps Local Area Networks (LANs) and Base Area Network (BAN) attached devices. The Base Area Network (BAN) service shall address the specific mission requirements of each site, with regard to security, functionality, classification, performance (such as latency within the BAN boundary and packet loss), survivability (including fault tolerance), interoperability, network management, and total bandwidth available to accommodate Navy and Marine Corps surge requirement.

Scope: Basic service for NMCI infrastructure, and external networks

Reference: SLA 25

3.3.3 Proxy and Caching Service

Requirement: The contractor shall provide the capability for caching and proxy to enhance information access and performance on both classified and non-classified networks.

Scope: Basic service for all data seats.

3.4 Systems Services

3.4.1 Network Management System (NMS) Service

Requirement: The contractor shall provide services that include Fault Management, Configuration Management/Asset Management, Account (empirical user data and fiscal accountability) Management, Performance Management, and Security Management. These services shall be provided in accordance with the Service Level Agreements. The contractor shall make available to designated Government entities, near real time information feeds to support Government oversight, maintain accessible historical data, provide summary management reports that detail the NMS functions, and allow the DoN to forecast its future networking requirements through the use of modeling techniques.

Scope: Basic service for all NMCI infrastructure and DoN organization

Reference: SLA 28

3.4.2 Operational Support Services (OSS)

Requirement: Network operations display shall be provided to authorized users on a real-time basis , indicating status of network assets allocated to them for mission support. The display shall be available to authorized users at any mission-critical seat and show performance status of the overall network and individual servers and routers. Capability to display separate Navy and Marine Corps performance status, status by theatre (CINCPAC or JFCOM), and status by Navy and Marine Corps base is part of basic service. The contractor shall provide services that include, but are not limited to, Data Backups and Recovery, Data Archiving, Routine Database Audits and Maintenance, Log Retrieval and Audits, Purging of Records, and Network Address Administration. The contractor shall support Government oversight, maintain accessible historical data, and provide summary management information that detail the OSS functions.

Scope: Basic service for all NMCI infrastructure and DoN organizations

Reference: SLA 29

3.4.3 Capacity Planning

Requirement: The contractor shall provide modeling capabilities to support the planning of changes to the NMCI infrastructure, specifically to estimate future volume, usage, and application characteristics, as well as integration of emerging technology and utilization of DISN provided as GFE.   The contractor shall also measure the degree of penetration that users are making into a network centric culture by providing visibility into metrics which show moving from phone to email to VTC to browser and web portals. The contractor shall provide age of data stores, when last updated or accessed, number of hits, number of repeat hits etc.   These capabilities shall include every component of NMCI (voice, video, and data), as well as periodic analysis of the network capacity and recommendations for future engineering changes, for Government review and approval and in accordance with the SLA.

Scope: Basic service for the NMCI infrastructure and external networks.

Reference: SLA 30

3.4.4 Domain Name Server (DNS)

Requirement: The contractor shall provide Domain Name Server (DNS) services that include the address resolution of Uniform Resource Locator (URL) to IP addresses. This capability shall include both internal Navy and Marine Corps URLs as well as external URLs. The services shall meet all functionality of the current Domain Name Server (DNS) service, to include flexible support for deployed units and retain the navy.mil and usmc.mil domain name conventions. The contractor shall manage the NMCI network addresses.

Scope: Basic service for the NMCI infrastructure.

Reference: SLA 31

3.4.5 Search Engine Services

Requirement: The contractor shall provide a service whereby NMCI users may search the contents of NMCI intranet web pages. The contractor shall provide the capability for web-crawling, site indexing, and an efficient search engine. The service shall exclude authoring of the web content and application development.

Scope: Basic service for NMCI infrastructure.

3.4.6 Data Reporting

Requirement: The Contractor shall electronically post the following information for on-line access by the PCO and personnel designated by the PCO. Reports shall be in contractor format. The contractor is encouraged to post data in a database format, with access via selectable report formats. At a minimum, the following data shall be provided:

Type	Title	Contents	Frequency
Service Levels	SLA Data Report	Data showing service levels provided for period	Monthly
Financial	Small Business Report	Data showing small business cumulatively and at 1st and at 2nd and 3rd tier use for period	Every six months
Financial	Small Business Report	Data showing small business who had previously supported DON workload and are integrated into NMCI	Every six months
Financial	Small Business Report	Data showing small business revenue down to a site specific level (i.e., the base zip code or phone area code region)	Every six months
	Order Status Report	Data shall include ordering office, order number, order date, order status, back order date, ordered amount due, date order created, order created by I.D., date order last modified, number of ordered products, ordered product, product number, quantity, order product status and unfilled orders status, quantity shipped, date shipped, quantity installed, and order price.	Monthly
	Asset and Credit Report and Asset Management Database	Data shall include description of asset, location of asset, quantity of asset, assessment line item number, date of assessment, plant property value, age, life cycle duration and cost, proposed/actual credit amount, delivery order number, deductive delivery order amount, line of accounting, funding document number, funding document description, delivery order description, commitment amount, obligation amount, and expenditure amount. See Attachment 9.	Monthly (maintained continuously)
	Incentive Report	Data shall include order or modification number, date and amount, description of incentive, date of audit, and date of incentive payment.	Monthly
Security	Incident Report	Data shall include any configuration changes, computer incidents, network incidents, INFOCON status, and intrusion detection reaction alert status.	Within 24 hours of incident
	~~Risk Assessment and~~ C&A Documentation	~~Attachment 4, Reference SOO, para 4.8, 4.10, 3.5.2~~ Data shall include the following: • System Security Authorization Agreement (SSAA) • Risk Assessments • Vulnerability Assessments • Risk Mitigation Plans • See Paragraph 4.10 and Attachment 4, Paragraph 1.1.2.2	~~Within 60 days after receipt of each ordered segment. Maintained current on a continuous basis.~~SSAA: Initial draft 30 days after placement of first order, second delivery 90 days after placement of first order, third delivery 180 days placement of first order, with revisions

			at IOC and FOC and if there are any significant architecture changes at any other time. All other requirements due annually, at a minimum.
	DISN Connection Approval Documentation	Data shall include documentation required for NIPRNET and SIPRNET connection approval as specified in DISN connection approval policy documents cited in Paragraph 4.10 and Attachment 4, Paragraph 1.1.2.2	30 days following placement of first order
	Security CONOPS (Including Disaster Recovery Plan)	Attachment 6 and Attachment 4, Paragraphs 1.1.2.2, 1.1.2.9, 1.1.2.10	Within ~~60 days after receipt of each ordered segment.~~45 days placement of first order and updates semi-annually thereafter. ~~Maintained current on a continuous basis.~~
	Security Critical Product Selection	Data shall include a listing of all IA mechanisms, to include but not be limited to the following: firewalls, intrusion detection systems, virtual private networks, security management tools, operating system for server and user workstations, smart card reader, etc.	15 days after placement of first order and within 10 working days of changes
	Security Status Report	Real time data feed supporting government oversight of security functions. See Paragraphs 3.5.1, 3.5.2, 4.4, 4.5, and Attachment 4 paragraphs 1.1.2.11, 1.1.3, and Attachment 6, paragraphs 5.7 and 5.8	Continuous
	Security Procedures	Data shall include security procedures describing how IA mechanisms will be operated to provide the security services specified in Paragraphs 3.5.1 and 3.5.2	Delivery with initial seats, updates with changes
	GFE Type 1 Crypto Requirements	Data shall include a detailed listing of required GFE Type 1 crypto devices. Data shall include the following at a minimum: quantity of Type 1 crypto required, classified key material required, dates required for both crypto and classified key material:	15 days placement of first order, updates with changes
Architecture	Diagram Reports	The documentation will provide a systems architecture view of the NMCI in contractor's standard format. The documentation will include a full description of all external interface points, to include DoD compliant technologies, protocols, and peering arrangements for external connectivity. It will include physical and logical connectivity, and how interoperability is achieved at the interfaces. The architecture will detail NMCI hosting of legacy systems. Data shall include graphic architecture designs and cabling diagrams, at least to the building level	NLT IOC, and within 5 working days of changes
	Network Connectivity Plan	Data shall include network topology showing WAN/MAN/BAN/LAN connectivity. All external interface connection points (DISN, Internet, etc.) shall be clearly annotated.	15 days placement of first order and within 10 working days of architecture changes
	Security Architecture	Data shall include architecture diagrams that depict how information is transferred through defense in depth boundaries 1 through 4 (e.g., from MAN/WAN connections at boundary 1 to interior destinations, down to hosts on LAN at boundary 4). Diagrams should include the	15 days placement of first order, and within 10

		proposed employment of all major network components (at a minimum in-line network encryptors, firewalls, intrusion detection systems, servers, routers, switches, load-balancers, and data path) which play a significant role in network operation, management, and security. Diagrams shall also indicate location of alternate paths and backup equipment. This includes information sources, supporting paths and capacities, any unique manipulation of data in transit, points of termination and placement of all proposed security components. The diagrams shall be in contractor format. Diagrams shall address both unclassified and classified architectures, and also any unique architectural differences associated with different types of locations (NOC, large base, small base, etc.). See Paragraph 4.5.	working days of architecture changes.
Transition Planning	Fielding and Transition Plan~~Implementation Report~~	Contractor shall generate a transition plan which will provide the means for coordinating system, product, and service rollouts and test with the Government in accordance with paragraph 3.6.2. This plan shall reflect ~~which will reflrect~~ the actions identified in the Risk Assessment, C&A, and Security CONOPS (including Disaster Recovery Plan) (as shown above), and Interoperability Test Plan, and shall be developed in conjunction with the Government Program Management Office for each orderable segment	Within 30 days after receipt of each ordered segment. To be updated on a monthly basis.
Embarkables	Consumable and Electronic Test Equipment Report	Data shall include a list of consumable items with sources, and a list of electronic test equipment	Updated with each deployed unit
Personnel	Personnel Skill Maintenance Plan	Data shall include a plan for affected personnel assignments and training monthly.	Monthly
Voice	Voice Billing Statements	Separate billing statements at the seat/line/trunk level for tolls on FTS 2001 or commercial long distance (2.2.3)	Monthly
Video	Configuration Management Report	Provide data sufficient to identify configuration management of video seats (2.3)	Updated with each deployed unit
Interoperability Document	OCONUS interoperability	Interoperability technical information for OCONUS provider (2.4)	As required
~~DISA~~ DISN Waiver	Request for Government Waiver	Waiver for commercial or alternative to DISA/WAN service (2.6)	As required
~~Security~~	~~Security Status Report~~	~~Real time data feed supporting government oversight of security functions (3.5.1, 3.5.2)~~	~~Continuous~~
~~Security~~	~~Security Procedures and Implementation Plans~~	~~Security procedures and implementation plans at user level, site licenses and server licenses (4.8)~~	~~Delivery for seat, updated as necessary~~
Network Management System Service	Information Feeds for Government Oversight	Historical data summary and management reports detailing NMS functions (3.4.1)	Continuous
Integrated Configuration Management	Logical Relationship Record	Logical relationship record of items and asset inventory (3.6.1)	24 hours after change

3.5 Information Assurance Services

3.5.1 NMCI Security Operational Services

Requirement: The contractor shall provide security services for protection of the Information Systems, Information System Domains (Communities of Interest), and Information Content (at rest, in use, and in-transit) in accordance with DoD, DoN, Navy, and Marine Corps Information Assurance policies and procedures. These security services shall be provided to protect both non-classified and classified information. These operational security services shall be fully integrated with the DoD PKI services to ensure confidentiality, integrity, availability, authenticity, and non-repudiation requirements as defined in the NMCI Security Requirements and Policy documents. The contractor shall implement the necessary information Assurance mechanisms to implement these security services, and shall conduct vulnerability assessments to validate that the necessary controls are in place to satisfy the IA requirements for NMCI. As part of implementing these security services the contractor shall be responsible for implementing

Government directed IA mandates such as INFOCONs (information operations conditions) and IAVAs (information assurance vulnerability alerts). Implementation of IA mandates shall be accomplished within Government specified timeframes. The contractor shall also be responsible for ensuring that the NMCI meets the requirements for certification and accreditation in accordance with DoD, DoN, Navy, and Marine Corps policy and SLAs (see Attachments 2, 4, and 5). As part of these security services, the contractor shall make available near-real time data feeds to support Government oversight detailing the security operational functions. For further definition of NMCI security operational services, the contractor shall comply with the NMCI Security Policy, NMCI Security Requirements document, Naval VPN Selection Criteria Document, and NMCI System Administrator's Training and Certification guidelines. The following security documents are provided for supporting information: NMCI Security Functions Concept of Operations (Attachment 6), NMCI Active Computer Network Defense Strategy: Cyber-Centric Maneuver Warfare (Attachment 11), and the DAA for the NMCI.

Scope: Basic for all NMCI Service Delivery Points and Services.

Reference: SLA 33

3.5.2 NMCI Security Planning Services

Requirement: These strategic security services shall provide for the NMCI to enhance the confidentiality, integrity, availability, authenticity, and non-repudiation requirements. The contractor shall support the use of mechanisms including, but not limited to, encryption, access control, user identification and authentication, malicious content detection, audit, and physical and environmental control. The contractor shall make available in accordance with the SLA, periodic information feeds to support Government oversight, maintain accessible historical data, and provide summary management reports that detail the security planning functions. The contractor shall conduct vulnerability assessments. At specified periods, the contractor shall propose updated/revised architecture designs to accommodate changing requirements, emerging technology, and results of vulnerability assessments, for Government review and approval.

Scope: Basic for all NMCI Service Delivery Points and Services.

Reference: SLA 36

3.6 Other Services

3.6.1 Integrated Configuration Management (CM)

Requirement: The NMCI contractor shall maintain a Configuration Management System including an asset inventory of all NMCI hardware and software (Attachment 9). In addition, the contractor shall maintain a logical relationship record of the items in the asset inventory. Changes to NMCI assets inventory shall be reflected in the configuration management system no later than 24 hours after the change. The logical relationship record shall reflect updates no more than one hour after the change.

Scope: Basic service for all data, voice and video seats, and for NMCI infrastructure and external networks.

3.6.2 Integration and Testing

Requirement: When the contractor modifies the user's existing configuration, (e. g., during initial seat fielding, applying maintenance or technology refreshment/insertion enhancements), the contractor shall:

(a) Minimize the time involved to complete the configuration modification to achieve the updated baseline.

(b) Test prior to deployment , ~~Test~~ and coordinate system, product, and service roll outs with the Government to facilitate implementation and to minimize impact to users. Coordination with the government shall include agreement on the scope of interoperability testing to be conducted in accordance with paragraph 3.6.4.

(c) Maintain interoperability amongst the various seat configurations. A modification to any existing baseline configuration, which was interoperable prior to the modification, shall maintain that interoperability after the modification is fully integrated.

(d) Maintain interoperability with extranets and relevant non-NMCI provided components of the DOD Global Information Grid.. Interoperability shall not be affected by any modification of the user's existing configuration~~enhancement~~.

At the Government's discretion, modifications to the baseline (e. g., evolving Standards and Architecture) and the integration of those modifications shall be required to be demonstrated to the Government prior to implementation.

Scope: Basic service for all data, voice and video seats, and for NMCI infrastructure and external networks.

3.6.3 Transition Planning Support

Requirement: The contractor shall provide NMCI transition planning support to DoN organizations. The planning will be limited to the migration of today's "as-is" information technology user systems to NMCI desired service level support.

Scope: Basic service for all service delivery points

3.6.4 Interoperability Test Plan

Requirement: The vendor shall develop an interoperability test plan and procedures that will minimizing the possibility of interoperability problems during modification of user existing configurations as discussed in paragraph 3.6.2, verifies that interoperability is intact upon completion of the modifications, and provides for interoperability monitoring during service provisioning.

As part of transition planning (paragraph 3.6.2), the government will provide, in government testing and evaluation plans, an Operational Architecture for the segment being installed and integrated or modified. This Operational Architecture will illustrate NMCI/ non NMCI information flows among selected facilities. The contractor shall ensure that interoperability between NMCI and and all existing non-NMCI GIG components including those defined in the OA, is maintained during the modification. The contractor's Interoperability Test Plan shall verify interoperability after segment installation and integration completion. As part of post modification testing, Interoperability Testing shall include, but is not limited to, a verification of the interoperability of the joint and DOD-wide applications from the list provided at 3.6.5 that are legacy to the segment being modified. The government testing and evaluation plans will define the applications from 3.6.5 and other critical applications that are legacy to the segment being installed and integrated or modified. The government providing of a list of critical applications for interoperability assurance and testing purposes does not alleviate the contractor of the contract requirement to maintain the interoperability of legacy applications.

~~The NMCI must comply with defined Joint Technical Architecture (JTA) and DoD and DON policies to ensure that all NMCI services are interoperable, both within NMCI and between NMCI and other networks. The vendor shall develop an interoperability test plan and procedures that support this particular service. This test plan provides~~ The Interoperability Test plan shall also provide for a series of mechanisms that detect unacceptable trends in performance that indicate that the software and hardware installed, component settings, and/or procedures are not in compliance, and must be corrected to support interoperability. This test plan shall address availability as it relates to the following services: Standard Office Automation Software, E-mail Services, Directory Services, Web Access Services, Newsgroup Services, NMCI Intranet Performance, NIPRNET Access, Internet Access, Mainframe Access, Desktop Access Government Applications, Unclassified Remote Access, Classified Remote Access, Organizational Messaging Services, Desktop VTC, Voice Communications, Wide Area Connectivity, BAN/LAN Communications Services, Moveable Video Teleconferencing Seat, Proxy and Caching Services, External Networks, SIPRNET, and Public Key Infrastructure (PKI).

The test plan reporting criteria shall include a threshold level, agreed to by Government and the vendor, that requires immediate notification of the Government and appropriate action by the vendor to correct. Corresponding SLAs are prescribed for these services and they stipulate response times to Government for exceeding these threshold levels and correcting NMCI related deficiencies. The test plan will be proposed by the offeror and approved by the Government for implementation in accordance with the appropriate SLAs.

References: SLA 2, 3, 4, 6, 7, 10, 11, 12, 13, 14, 18, 19, 20A, 21, 22, 24, 25, 26, 26A, 27, 34, ~~and~~ 35, and 3.6.5 of this document.

3.6.5 Critical Joint Applications

Community of Interest	OPR	System Identification
Logistics		
	DLA	Fuels Automated System (FAS)
	DLA	DoD Standard Procurement System (SPS)
	DLA	Defense Property Accountability System
	DLA	Distribution Standard System
	DLA	Subsistence Total Order & Receipt Electronic System
	DLA	Client Server Initiative(DSS Rehost)
	DLA	Defense Integrated Subsistence….
	DLA	Defense Reutilization and marketing
	DLA?	Joint Total Asset Visibility (JTAV)
	Army	Joint Computer Aided Logistics (JCALS)

	Army	Transportation Coordinators Automated Information for Movements System (TC-AIMS II)
	Navy	Joint Engineering Data Management Info system (JEDMICS)
	Navy	Material Management System
	Navy	Configuration Management Information System
	Air Force	Ammunition Management Standard System (AMSS)
	Air Force	Stock Control System
	TRANSCOM	Global Air Transportation Execution System
	TRANSCOM	CONUS Freight Management System
	TRANSCOM	World Wide Port System
	TRANSCOM	Core Automated Maintenance System
	TRANSCOM	Global Transportation Network
Health		
	OSD-HA	Composite Health Care System II (CHCS II)
	OSD-HA	Theater Medical Information System (TMIP)
	OSD-HA	Defense Medical Logistics Standard Support System (DMLSS)
	OSD-HA	Corporate Executive Information System
	OSD-HA	Health Standard Resources System
	TRANSCOM	Transcom (Medical) Regulating C2
C2		
	DISA	Global Combat Support System (GCSS)
	DISA	Global Command and Control System (GCCS)
	Transcom	Command and Control Information Processing System (C2IPS)
Finance		
	OSD-C	Defense Travel Service (DTS)
	DFAS	Defense Working Capital Accounting System (DWAS)
	DFAS	Defense Joint Military Pay System (DJMS)
	DFAS	Defense Joint Accounting System (DJAS)
	DFAS	Defense Procurement Payment System (DPPS)
	DFAS	Standard Accounting & Reporting System (STARS)
	DFAS	Defense Civilian Payroll System (DCPS)
	DFAS	Defense Industrial Financial Management System (DIFMS)
	DFAS	Defense Standard Disbursing System (DSDS)
	DFAS	Defense Business Management System (DBMS)
	DFAS	Standard Accounting Budgeting & Reporting System (SABRS)
	DFAS	General Accounting and Finance System - Reengineered (GAFS-R)
P&R		
	Navy	Defense Integrated Military Human Resources System (DIMHRS)
	Air Force	Defense Civilian Personnel Data System
	DHRS	Defense Enrollment Eligibility Reporting System
	TBD	JPAS
Intell		
	DIA	Joint Intelligence Virtual Architecture (JIVA)
	NIMA	U.S. Imagery & Geospatial System (USIGS)
	NIMA	National Exploitation System (NES)
	NIMA	Requirements Management System (RMS)

IM/M&S

DISA	Defense Messaging System (DMS)
Navy	Joint Simulations System (JSIMS)
Joint Staff	Joint Simulation System
Joint Staff	JCS Joint Modeling and Simulation
DTRA	Compliance Monitoring and Tracking System
DTRA	Data Archival and Retrieval Enhancement System
TRANSCOM	Global Decision Support System

3.7 Additional Requirements for Embarkable Seats

Requirement: The contractor shall provide embarkable equipment meeting the technical description and compatibility requirements defined in Interface Control Document.

Survivability: The embarkable seat shall provide sufficient shock protection for Naval and Marine Corps expeditionary use and for ship, air, and vehicle transportation modes.

The NMCI contractor shall supply a number of spares to facilitate operation at sea. The contractor shall use as a basis for evaluation of required spares and ILS support the projected equipment as described below.

Embarkable Equipment Support During Deployment: The contractor shall provide worldwide support for deployed equipment and software to meet the Specified availability in SLA 1 (Attachment 2).

Equipment support methods used to meet the specified availability may include, but are not limited to, pre-positioning of spares, deploying replacement units, using forward "points of service", provide on-line troubleshooting, or the use of deployed Naval/Marine Corps maintainers. The contractor may require certification of those Government individuals allowed to perform equipment maintenance. Any required training and certification of Government personnel to perform maintenance shall be provided at no cost to the Government.

Equipment failing while embarked will be handled by the Government in accordance with contractor/Government approved technical documentation. Deployed users or their support infrastructure will obtain a Return Material Authorization (RMA) from the contractor prior to returning hardware. The contractor shall ship parts via a commercial package delivery carrier, registered mail, or any other means considered acceptable to both the contractor and the Government. The contractor shall be responsible for all costs associated with the commercial shipment. The mode and priority of shipment shall support the specified availability.

Equipment Identification: The contractor shall label embarkable equipment with information identifying the equipment as NMCI, and include sufficient information to facilitate inventory management and disposition of failed items by both the Government and contractor. This attached label shall be durable enough to last through the life of the material.

Hardware Refurbishment: The contractor shall perform preventive or corrective maintenance upon return of the embarked units and prior to reconnection with the shore NMCI infrastructure. The maintenance function shall include, but is not limited to reconfiguration or upgrades of software and hardware necessary ensure NMCI compatibility. The contractor shall identify damage of returned equipment, and shall store equipment for Government inspection.

Configuration Management: In addition to the Configuration Management provisions for all NMCI equipment and software, the contractor shall provide the additional configuration management information required by Attachment 9.

Technical Documentation: The contractor shall provide OEM manuals and supplemental technical information necessary to support the existing configuration. The contractor shall also provide the processes for obtaining supply sources and maintenance information for the deployable units as well as troubleshooting and casualty control procedures as part of the technical documentation. It is preferred that this information be provided in electronic format for ease of transport.

Training: The contractor shall conduct analysis to identify user level differences in the operation of NMCI and IT-21. The contractor shall develop any needed curricula maximizing use of existing training capabilities to train embarkees in the use of NMCI equipment in embarked environments. These curricula shall be available electronically for use by NMCI user community.

Support Equipment: Should the contractor approach to support of embarkables include contractor-certified Naval/Marine Corps maintainers, the identified ETE shall be provided at no additional charge to the Government, in quantities to support the specified availability.

NMCI embarkable workstations/embarkable portables shall be capable of interfacing with and being reconfigured for compatibility with IT-21 shipboard networks as described below as well as the Marine Corps Tactical Network (MCTN) as described in Attachment 10. Reconfiguration of NMCI embarkable workstations/embarkable portables (and required software licenses) to interface with IT-21 or other non-NMCI (e.g. disembarked) networks is not the responsibility of the Contractor. Reconfiguration of NMCI embarkable workstations/embarkable portables (and required software licenses) for return and interface with NMCI is the responsibility of the Contractor. Preservation of user data during re-configuration and return to NMCI is required.

Minimum requirements for NMCI embarkable workstations/laptops to be embarked on IT-21 platforms: NMCI workstations/laptops shall meet or exceed current IT-21 hardware standards at the time of delivery, and be re-configurable to support current IT-21 COTS/GOTS applications.

USS John C Stennis/USS Bon Homme Richard Networking Guidebook Version 0.93 13 October 1999 lists the current COTS/GOTS applications and versions:

Application	**Version**
Windows NT	4.0 workstation -- Service Pack 4 with hotfixes
MS Office	97 Professional -- Service Release 2
MS Exchange/Outlook	98

MS Internet Explorer	4.0 or later
Netscape Communicator	4.0 or later
Norton Anti-virus	5.0 (from DoD contract)
MS Office Draw	97 (freeware)
WinZip	6.3 or later
MS BackOffice client license	
MS Net Meeting	2.1 (freeware)
MS GIF animator	1.0 (freeware)
Disk Keeper Lite	2.0 (freeware)
JMHS client applications	
Common Message Processor (CMP)	

Current IT-21 hardware specifications (Per recent IT-21 program purchases):

Workstations	Laptops
400Mhz Pentium II CPU	300Mhz Pentium II CPU
64MB RAM	64MB RAM
512K cache	32K Level 1 cache - 128K Level 2 cache
8MB Video RAM	2.5MB Video RAM
6.4GB hard disk drive	4.1GB hard disk drive
1.44MB 3.5" floppy disk drive	1.44MB 3.5" floppy disk drive
32x CD-ROM	24x CD-ROM
Keyboard	Integrated 56K V.90 modem
Mouse	Pointing device
Sound Blaster Pro compatible audio card with speakers and microphone	Sound Blaster Pro compatible audio card
17" monitor	13.3" Active Matrix Color
SMC 10/100 Base-T or FL NIC or 3COM ATMLINK PCI 155MB ATM OC-3 NIC	SMC 10/100 Base-T PCMCIA NIC

Scope: Basic for embarkables

4.0 Information Assurance/Computer Network Defense (IA/CND) Requirements

Scope: Basic service for all data seats, fixed and secure voice devices, video teleconferencing seats, NMCI infrastructure, and external networks.
Reference: SLA 33, 34, 35, 36

4.1 General DoD and DoN IA Policies

As specified in DoDD 5200.28 (Security Requirements for Automated Information Systems (AISs), DoDI 5200.40 (DoD Information Technology Security Certification and Accreditation Process - DITSCAP), SECNAVINST 5239.3, OPNAVINST 5239.1B, and DoD 5200.2-R, all automated systems shall meet fundamental security requirements and must be accredited by the Designated Approving Authority (DAA) prior to processing classified or sensitive non-classified data. The NMCI shall be implemented with proper products, policies, and procedures to ensure required system C&A in accordance with this policy. Also, the specific IA guidelines specified in CNO ALCOM 081949Z SEP 99, DoN CIO ITIA, and DoN ITSG shall be implemented within the NMCI.

Reference: SLA 33

4.2 Public Key Infrastructure (PKI)

As specified in DEPSECDEF Memo dtd 09 Apr 1999, DoD PKI Implementation, any PKI employed within DoD Services and Agencies shall be the DoD PKI. Thus, the NMCI shall incorporate DoD PKI in accordance with the following guidelines. Specifically, the high assurance PKI based in FORTEZZA and the medium assurance PKI based on X.509 Version 3 certificates shall be used within NMCI. The Government will provide the Contractor with the DoD PKI user profile as GFI to be implemented within NMCI. The Contractor shall support the medium assurance PKI implementation of smart cards. In accordance with DEPSECDEF memo dtd 10 November 1999, the primary carrier of the DoD medium assurance PKI credentials will be the Common Access Card (CAC), a smart card. The CAC will be issued by DEERS/RAPIDS to all DoD active duty military, selected reserve military, civilians, and seated contractors, DoD Total Force. CAC issuance will commence October 2000 with DON Total Force completed by 1st Quarter FY02. Prior to this, the DoN will issue an alternative smart card for the purposes of network logon, digital signature, etc. In accordance with this policy, all PKI enabled applications for the NMCI must be compatible with the DoD PKI, and authorized DoD certificate authorities must issue all certificates. The Contractor shall perform PKI management functions, including user registration and derived key management in accordance with Paragraph 3.1.16 above. Based on this policy, the NMCI shall be able to support the following:

a. The contractor shall use only DoD Public Key Infrastructure (PKI)-enabled servers.
b. The contractor shall provide digital signature capability for all electronic mail services implemented. The DoD PKI credentials will be residing on the CAC or equivalent DoN provided smart card.
c. The contractor shall register all users . This shall include registration, facilitation of the issuance of identity and email certificates (signature and confidentiality)(as required)(LRA functions) This shall also include management of user PKI certificates: including certificate revocation, tracking and implementation. The registration functions shall be performed to the extent necessary to augment the DEERS/RAPIDS-LRA capability to provide all required PKI LRA and management functions for users (personnel, servers, objects, devices, etc.)d. The contractor shall provide user training for DoD PKI certificate use.
e. The contractor shall register servers and install DoD PKI server certificates for PKI enabled applications DoD PKI certificates will be used for client-server identification and authentication for all private DoD and DoD-interest web servers on both classified and unclassified networks.

Reference: SLA 34

4.3 Multi-Level Security (MLS)

Any implementation within the NMCI of a MLS device such as a High Assurance Guard or MLS Web Server shall be in accordance with the guidelines established by the Defense Information Switch Network (DISN) Security Accreditation Working Group (DSAWG) and the Secret and Below Interoperability (SABI) effort. Accordingly, in cases where the NMCI is required to interface with Coalition networks, use of a Type 1 cryptographic device is required.

4.4 Computer Network Defense (CND)

Implementation of NMCI shall be consistent with current DoN Computer Incident Reporting guidelines included in OPNAVINST 2201.2 dated 3 March 98, Navy and Marine Corps Computer Network Incident Response. Also, network availability and security information from the entire NMCI shall be made available to the DoN components of the DoD Joint Task Force for Computer Network Defense (JTF-CND), so that analysis can be performed across regions and network defense strategies can be coordinated across the DoN. The DoN components of JTF-CND will work with the other elements of JTF-CND to coordinate network defense across DoD and the U. S. Government as a whole.

4.5 Critical Government Roles with respect to IA/CND

Although DoN expects the Contractor to pursue an aggressive strategy for design, deployment, and operation of the NMCI, authorized DoN personnel must perform a number of critical security roles. These roles fall into two categories: insuring that the security of the NMCI satisfies DoN, DoD, and Federal requirements and exercising essential command authority over DoN defensive Information Warfare (IW) activities.

The contractor shall be required to establish CMS accounts in accordance with the National Industrial Security Program Manual (NISPM). The Government will furnish cryptographic equipment and keying material. The contractor shall be responsible for loading the keying material into the cryptographic equipment used to protect information classified at SECRET or below, using the Electronic Key Management System (EKMS) as appropriate. The contractor shall be accountable for all CMS material in accordance with the National Industrial Security Program Manual (NISPM). The contractor shall be responsible for all shipping and handling of GFE NMCI cryptographic material to and from a DoN Crypto Repair Facility (CRF) for required depot repairs.

In concert with the requirements for Certification and Accreditation (C&A) of all DoD computer networks (classified and non-classified), authorized DoN personnel under the direction of the certification authority shall be the approving authority for the following components of the NMCI:

a. Security Architecture
b. Security critical product selections
c. Network connectivity plan
d. Security procedures
e. Other security critical factors as required

In the above role, DoN personnel will seek to use the most expeditious procedures without compromising the integrity of the security evaluation process. Also, with respect to item (b) above, the NMCI shall comply with the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 for the implementation of COTS and GOTS products IA and IA-enabled IT products.

DoN will use security assessment teams (Red and Green Teams) to conduct authorized simulated attacks against operational NMCI networks to ensure the NMCI satisfies the security related SLAs and that Navy, Marine Corps, DoN, DoD, and national security requirements are adhered to. As part of this approach, Red/Green Teams will also conduct design, product, and configuration reviews. Focus of Green Teams will be on contract related security requirements, while Red Teams will be less constrained and will focus on identifying vulnerabilities and risk associated with operation of the NMCI. DoN will ensure that Navy, Marine Corps, DoN, DoD, and national policies and procedures are followed in conducting Green/Red Team operations. While DoN intends to use contractor support personnel to supplement government personnel in conducting security assessment operations, leadership of these teams shall be government based.

With respect to CND, responses to network threats and attacks constitute Information Warfare (IW) defense command decisions that as a minimum shall be authorized by designated DoN personnel. Along this line, the DoN command structure shall retain directive authority over all NMCI threat responses. These DoN personnel shall also be the conduits for authorized responses to directives received from JTF-CND or Joint Service regional CINCs, for coordinated Joint Service response to threats. In particular, as the INFOCON level is raised, DoN personnel shall retain command decision authority. During these periods, SLA compliance may be relaxed at the sole discretion of the PCO.

DoN shall be the approving authority for the security architecture since government personnel will be responsible for security critical roles and shall have to use the infrastructure for critical operations. The security architecture is the primary mechanism that underlies the criticality of the NMCI. The overall performance of the network shall still be the responsibility of the contractor given this constraint.

DoN personnel will retain only essential command authority and approval authority of security significant changes. With the constraints outlined above, the contractor is still responsible for the overall performance of the NMCI in accordance with the SLAs.

4.6 Secure Voice Interface

The NMCI shall provide for interfaces to existing secure voice systems, specifically for interoperability with Type 1 Secure Voice products, specifically, the NMCI shall provide interfaces to STU-III/STE for joint/allied interoperability. The NMCI shall be able to bridge to existing infrastructures to ensure ship to shore secure voice interoperability. Ref: ITIA 4.12.

4.6.1 NMCI Security Planning Services

These security strategic services shall provide for the NMCI to enhance the confidentiality, integrity, availability, authenticity, and non-repudiation requirements. The contractor shall support the use of appropriate mechanisms including, but not limited to, encryption, access control, user identification and authentication, malicious content detection, audit, and physical and environmental control.

Scope: Basic service for all data, voice, and video seats

Reference: SLA 36

4.6.2 SIPRNET Access

The contractor shall provide point(s) of entry for each data seat to access the SIPRNET.

Scope:	Basic service for classified Connectivity Upgrade Package (HW), Clin 0009 (and 0109 if option is exercised)

Reference: SLA 35

4.7 Classified (DoD) Information Support

The highest classification level of information required in connection with this procurement is SECRET. Since Top Secret data may be tunneled over NMCI using Type 1 encryption, the NMCI shall be required to accommodate this capability. Thus, NMCI shall be able to interface with Top Secret enclaves where required and provide a capability to transport Top Secret data using certified and accredited separation mechanisms such as Type 1 cryptographic products.

In accordance with the National Industrial Security Program Operating Manual, DoD 5220.M, the contractor must possess or be able to possess a Facility Security Clearance equal to the highest level of classified information necessary to perform the tasks or services required on this contract. Security requirements relating to the handling and safeguarding of classified information are identified in DD Form 254 (Attachment 7). Contractor personnel, whose duties require access to systems processing classified information, must possess a security clearance at least equal to the highest degree of classification involved (SECRET) and have a validated need-to-know prior to beginning work on the classified system. The sponsoring agency's security requirements for classified systems must be met by all contractor personnel accessing classified information or systems processing classified information.

4.8 Sensitive Information Support (Non-Classified)

Under current Federal guidelines, all officially held information is considered sensitive to some degree and must be protected by the contractor as specified in applicable IT Security Plans. Types of sensitive information that will be found on DoN systems include: Privacy Act information, information that is proprietary to companies or contractors other than the subject contractor, resources protected by International Traffic in Arms Regulation (ITAR), technology restricted from foreign dissemination, DoN administrative communications, including those of senior Government officials, procurement or budget data, information on pending cases by Equal Employment Opportunity (EEO), labor relations, legal actions, disciplinary actions, complaints, IT security pending cases, civil and criminal investigations, information not releasable under the Freedom of Information Act (FOIA) (e.g. payroll, personnel, and medical data).

The contractor shall perform internal assessments to determine position sensitivity and management controls necessary to prevent individuals from bypassing controls and processes, such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges at contractor facilities. These position sensitivity assessments shall be forwarded to the Government for a determination of personnel suitability and requirements for individuals assigned to these positions. Periodic re-evaluations of positions and suitability requirements shall be necessary during the life of the contract as positions and assignments change.

Performance under this contract will involve access to and/or generation of sensitive information or systems. The contractor shall perform an assessment to determine position sensitivity and management controls to prevent the individuals in these positions from bypassing controls and processes such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges. Ongoing reevaluations of the position and suitability requirements will be necessary during the life of the contract as positions and assignments change.

The contractor shall conduct risk assessments, document the results, develop and maintain internal security plans. These plans shall describe how the contractor will ensure the integrity, availability, and confidentiality of the information that is operationally responsible to protect within the vendor’s facilities and at government facilities. For example the contractor shall ensure that foreign nationals within their corporate staff shall not have access to NMCI data that is not releasable. A decision to accept any residual risk will be the responsibility of the DoN system owner and the DoN information owners. The contractors risk assessments and IT Security Plans shall be updated at least every three years or upon significant change to the functionality of the assets, network connectivity, or mission of the system, whichever comes first. If new or unanticipated threats or hazards are discovered by the contractor, or if existing safeguards have ceased to function effectively, the contractor shall update the risk assessments and IT Security Plans (within 30 working days) and shall make risk reduction recommendations to the DoN system owner and the DoN information owners (within 5 working days).

4.9 Privacy and Security Safeguards

The contractor shall not publish or disclose in any manner, without written consent of the Government the details of any security safeguards designed, developed, or implemented by the contractor under this contract.

The contractor shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user, such as being reassigned, removed for repair, replaced, or upgraded, is cleared of all DoN data and sensitive application software by a technique approved by the Government, currently overwriting at least three times. For IT resources leaving DoN use, applications acquired via a "site-license" or "server license" shall be removed. Damaged IT storage media shall be degaussed or destroyed.

To the extent required to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of Government data, the contractor shall afford DoN access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, databases, and personnel. Government will conduct an audit on an aperiodic event-driven basis the of contractor’s CMS accounts.

4.10 Certification and Accreditation (C&A)

The Government will provide the NMCI contractor with the most current information regarding the C&A status of the existing DoN networks that comprise the “as is” configuration of the NMCI. The NMCI contractor shall be responsible for developing a transition plan to support the migration from the “as is” NMCI at contract award to the contractor implemented NMCI. The NMCI contractor shall be responsible for delivering a system that can be certified and accredited in accordance with NMCI Security Requirements (Attachment 4) and NMCI Security Policy (Attachment 5). With this support, the NMCI contractor shall support the Government in the following phases of C&A as defined in the DITSCAP: Definition, Verification, Validation, and Post-Accreditation. This accreditation is an essential part of the connection approval process (CAP) for DVS-G, NIPRNET and SIPRNET. The contractor shall be responsible for supporting the Government in satisfying the requirements specified in DISA MSG DTG021730Z subject DISN NON-CLASSIFIED BUT SENSITIVE INTERNET PROTOCOL ROUTER NETWORK (NIPRNET) CONNECTION APPROVAL PROCESS. Similarly, the contractor shall be responsible for supporting the Government in satisfying the DISA (DITSCAP) requirements for connection to the SIPRNET(dated 20 August 1998) and the DISN Video Services Global. This shall include providing a security concept of operations document, sufficient architecture documentation, a system security authorization agreement (SSAA), risk assessments, risk mitigation plans, and other supporting documents required to support DITSCAP accreditation. The NMCI Contractor shall support the DoN in the role as certification agent.

4.11 NMCI Enclaves

A Community of Interest (COI) is a logical grouping of users who have a requirement to access information that should not be made available to the general NMCI user population. This requirement can be based on specific security requirements, geographical location, unique functional requirements, or unique command relationships. To meet this requirement, a logical perimeter is established around the COI, using Defense in Depth IA mechanisms. Some examples of COIs are personnel systems (for handling Privacy Act Data), geographically dispersed major claimants, and commands and shipyards handling nuclear propulsion data. COIs will be established under the authority of the NMCI Governance and Operations Organization.

The NMCI contractor shall dynamically establish, maintain, and disestablish multiple communities whose membership is dependent upon the presentation of community (enclave) credentials (PKI/keys), as required by and in coordination with the Government. All of the communities above the non-classified level require Type 1 cryptographic separation. However, the DAA may authorize the use of PKI and VPN technology for COI implementation within classified enclaves, as long as PKI and VPNs are not the primary mechanisms used to provide security services. Communities within non-classified enclaves require the use of PKI and VPN technology for cryptographic separation. Coalition isolation requires releasable cryptographic separation as determined by Government. Connection between communities requires a Government approved gateway or guard appliance. See NMCI Security Requirements (Attachment 4) and NMCI Security Policy (Attachment 5) for NMCI security requirements regarding required enclaves within the NMCI.

Some communities of interest (e.g., the USMC) will require the NMCI architecture to provide a separate enclave that rides the overarching NMCI. These community of interest enclaves will be established to allow security management and operational direction and will be separated from NMCI at large through boundary 2 firewall suites. These boundary 2 firewalls will enable implementation of a security domain, similar to establishing a service-wide community of interest, and will support implementation of unique security requirements. Boundary 2 firewall suites providing this function will mirror the NMCI solution for meeting boundary 1 security requirements.